ACADEMIC PRESS

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Combinatorial Theory, Series A 101 (2003) 281–284

Journal of Combinatorial Theory Series A

http://www.elsevier.com/locate/jcta

Note

On $(2n, 2, 2n, n)$ relative difference sets

Yutaka Hiramine

Department of Mathematics, Faculty of Education, Kumamoto University, Kurokami, Kumamoto, Japan

Received 20 June 2002

Abstract

In this article, we show that a $(2n, 2, 2n, n)$ relative difference set in a group G of order $4n$ exists only if a Sylow 2-subgroup of G is non-cyclic and n is even unless $n = 1$. We also construct $(2n, 2, 2n, n)$ relative difference sets relative to non-normal subgroups.

1. Introduction

An (m, u, k, λ) *relative difference set* (RDS) in a group G relative to a subgroup U of order u and index m is a k-element subset R of G such that every element $g \in G \backslash U$ has exactly λ representations $g = r_1 r_2^{-1}$ with $r_1, r_2 \in R$ and no non-identity element of U has such a representation. The subgroup U is often called the *forbidden* subgroup. If $u = 1$, then R is an (m, k, λ) *difference set* (DS) in the usual sense. A $(u\lambda, u, u\lambda, \lambda)$RDS is called *semiregular*. An RDS R in a group G relative to a subgroup U is semiregular if and only if R is a complete set of right coset representatives of G/U.

Let R be a $(2n, 2, 2n, n)$RDS in a group G of order $4n$ relative to a *normal* subgroup $U \simeq \mathbb{Z}_2$ of G. Such a group is called *an Hadamard group* of order $4n$ by Ito [4]. In this article, we remove the condition that the forbidden subgroup is normal and show that a Sylow 2-subgroup of G is non-cyclic and n is even unless $n = 1$. We also give examples of RDSs relative to non-normal forbidden subgroups.

For a subset X of G, we set $X^{(-1)} = \{x^{-1} \mid x \in X\}$ and we identify a subset X of G with a group ring element $\hat{X} = \sum_{x \in X} x \in \mathbb{C}[G]$. Moreover, for $f = \sum_{x \in G} a_x x \in \mathbb{C}[G]$ $(a_x \in \mathbb{C},\ \forall x \in G)$, we set $f^{(-1)} = \sum_{x \in G} a_x x^{-1} \in \mathbb{C}[G]$. The terminologies are taken from [2,5].

E-mail address: hiramine@gpo.kumamoto-u.ac.jp.

0097-3165/03/$ - see front matter
doi:10.1016/S0097-3165(02)00013-4

2. The case that a Sylow 2-subgroup is cyclic

In this section, we show the following.

Theorem 2.1. *If a group G of order $4n$ contains a $(2n, 2, 2n, n)$RDS, then a Sylow 2-subgroup of G is non-cyclic and n is even unless $n = 1$.*

Proof. Assume n is even and a Sylow 2-subgroup of G is cyclic. In his paper [4], Ito showed the non-existence of $(2n, 2, 2n, n)$RDS in G relative to a normal subgroup U of G of order 2 (see [4, Proposition 7]). However, his proof does not depend on the normality of U. Thus, the theorem holds in this case.

Assume n is odd. If there is an element x of order 2 outside U, then x is represented even times as a difference $d_1 d_2^{-1}$ with $d_1, d_2 \in R$ because $x = x^{-1}$. This is contrary to $2n$. Hence, U contains all involutions of G and so $G \rhd U$. By Ito [4], $n = 1$. Thus, we have the theorem. □

By Theorem 2.1, $PSL(2, q)$ with $q \equiv 3, 5 \pmod 8$ contains no $(2n, 2, 2n, n)$RDS. We ask the following:

Question. Is there any finite simple group of order $8m$ that contains a $(4m, 2, 4m, 2m)$ RDS?

3. Construction of $(2n, 2, 2n, n)$RDSs

In this section, we give examples of groups that contain $(2n, 2, 2n, n)$RDSs relative to *non-normal* forbidden subgroups.

Throughout this section we assume the following:

Hypothesis 3.1. *Let R be a $(2n, 2, 2n, n)$RDS in a group G of order $4n(>4)$ relative to a subgroup $\langle t \rangle$ of order 2. There exists a normal subgroup N of G of index 2 such that $G = \langle t \rangle N$. Set $R = A + Bt$, where A and B are subsets of N. We may assume $|A| \leqslant |B|$ by exchanging R for Rt if necessary.*

Proposition 3.2. *Let notations be as in Hypothesis* 3.1. *The following hold*:

(i) *there exists a positive integer m such that $n = 2m^2$ and $|N| = 4m^2, |A| = 2m^2 - m$,*
(ii) $AA^{(-1)} + A^t(A^t)^{(-1)} = 2(m^2 + (m^2 - m)N)$, *where $A^t = t^{-1}At$, and*
(iii) $B = N \backslash A^t$.

Conversely, if a subset A of N satisfies (i) *and* (ii), *then a subset R of G defined by $R = A + (N - A^t)t$ is a $(4m^2, 2, 4m^2, 2m^2)$RDS.*

Proof. By assumption, $RR^{(-1)} = 2n + n(N + Nt - 1 - t)$. On the other hand, $RR^{(-1)} = (A + Bt)(A^{(-1)} + tB^{(-1)}) = (AA^{(-1)} + BB^{(-1)}) + (B(A^t)^{(-1)} + A(B^t)^{(-1)})t$. Hence we have

$$AA^{(-1)} + BB^{(-1)} = 2n + n(N - 1) \tag{1}$$

and

$$B(A^t)^{(-1)} + A(B^t)^{(-1)} = n(N - 1). \tag{2}$$

By (2), $A^t \cap B = \phi$. On the other hand, $|A| + |B| = |R| = |N| = 2n$ and $A^t, B \subset N$. Hence (iii) holds.

Set $a = |A|$ and $b = |B|$. Then, by (1) and (2), $a + b = 2n$ and $2ab = n(2n - 1)$. From this, we have $a = n - \sqrt{\frac{n}{2}}$ and $b = n + \sqrt{\frac{n}{2}}$. Set $m = \sqrt{\frac{n}{2}}$. Then $n = 2m^2$ and $|A| = 2m^2 - m, |B| = 2m^2 + m$. Thus (i) holds.

By (iii) and Eq. (1), we have $AA^{(-1)} + (N - A^t)(N - (A^t)^{(-1)}) = 4m^2 + 2m^2(N - 1)$. It follows that $AA^{(-1)} + A^t(A^t)^{(-1)} + (4m^2 - 2(2m^2 - m))N = 2m^2 + 2mN$. Thus (ii) holds.

Assume that a subset A of N satisfies (i) and (ii) and set $B = N \backslash (A^t)$. Then, one can easily verify that $(A + Bt)(A^{(-1)} + tB^{(-1)}) = 4m^2 + 2m^2(N\langle t \rangle - \langle t \rangle)$. Thus, $R(= A + Bt)$ is a $(4m^2, 2, 4m^2, 2m^2)$RDS relative to $\langle t \rangle$.

A $(4s^2, 2s^2 + \varepsilon s, s^2 + \varepsilon s)$ DS ($\varepsilon = \pm 1$) is called an *Hadamard difference set* of order s^2. □

Example 3.3. Let $N = \langle x \rangle \simeq \mathbb{Z}_{16}$ and let t_ε ($\varepsilon = \pm 1$) be an automorphism of N of order 2 defined by $x^{t_\varepsilon} = x^{8+\varepsilon}$. Set $A = \{1, x, x^3, x^4, x^5, x^{11}\}$ and $B = N \backslash A^t$, where $t = t_\varepsilon$. Then one can verify that A with $m = 2$ satisfies (i) and (ii) of Proposition 3.2. This implies that the semi-dihedral group SD_{32} of order 32 and the modular 2-group $M_5(2)$ of order 32 have $(16, 2, 16, 8)$RDSs relative to a non-normal subgroup of order 2 (see [3]).

If t leaves $AA^{(-1)}$ invariant in Proposition 3.2, then we have the following:

Proposition 3.4. *Let A be an Hadamard difference set of order m^2 in a group N of order $4m^2$ and $\langle t \rangle$ a group of order 2 operating on N as an automorphism group of N. Let $G = N\langle t \rangle$ be a semidirect product of N by $\langle t \rangle$. Then $R = A \cup (N \backslash A^t)t$ is a $(4m^2, 2, 4m^2, 2m^2)$RDS in G relative to $\langle t \rangle$.*

Proof. As $AA^{(-1)} = m^2 + (m^2 - m)N$, $A^t(A^t)^{(-1)} = m^2 + (m^2 - m)N$. Hence, A satisfies (i) and (ii) of Proposition 3.2. Therefore, $R = A + (N - A^t)t$ is a $(4m^2, 2, 4m^2, 2m^2)$RDS in G relative to $\langle t \rangle$.

In [1], Arasu et al. constructed a $(2n, 2, 2n, n)$RDS in a group $Z_2 \times N$, where N is a group of order $2n$ containing an Hadamard difference set. The above proposition can be regarded as a slight generalization of their result. □

Example 3.5. Let X be a group of order 4 and set $D = \{1\}(\subset X)$. Then D is an Hadamard difference set of order 1. Assume that a group $\langle y \rangle$ of order 2 operates on X. By Proposition 3.4, the following hold.

(i) If $X = \langle x_1, x_2 \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ and y centralizes X, then $\{1\} \cup \{x_1, x_2, x_1x_2\}y$ is a $(4,2,4,2)RDS$ in $\langle x_1, x_2, y \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ relative to $\langle y \rangle$.

(ii) If $X = \langle x \rangle \simeq \mathbb{Z}_4$ and y centralizes X, then $\{1\} \cup \{x, x^2, x^3\}y$ is a $(4,2,4,2)RDS$ in $\langle x, y \rangle \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$ relative to $\langle y \rangle$.

(iii) If $X = \langle x \rangle \simeq \mathbb{Z}_4$ and y inverts X, then $\{1\} \cup \{x, x^2, x^3\}y$ is a $(4,2,4,2)RDS$ in $\langle x, y \rangle \simeq D_8$.

Acknowledgments

We thank referees for several helpful comments and a shorter proof of Theorem 2.1.

References

[1] K.T. Arasu, D. Jungnickel, S.L. Ma, A. Pott, Relative difference sets with $n = 2$, Discrete Math. 147 (1995) 1–17.
[2] D. Gorenstein, Finite Groups, Harper & Row, New York, 1968.
[3] Y. Hiramine, Semiregular relative difference sets in 2-groups containing a cyclic subgroup of index 2, J. Combin. Theory, Ser. A 99 (2002) 358–370.
[4] N. Ito, On Hadamard groups, J. Algebra 168 (1994) 981–987.
[5] A. Pott, Finite Geometry and Character Theory, in: Lecture Notes in Mathematics, Vol. 1601, Springer, Berlin, 1995.